PC Security

When you connect to the Internet, allow other people to use your computer, or share files with others, you should take steps to protect your computer from a harm اذى. Why? Because there are computer criminals (sometimes called hackers) who attack other people's computers. These people can *attack directly, by breaking into your computer through the Internet and stealing your personal information, or indirectly, by creating malicious* خبيثة *software to harm your computer*.

Protect your computer

There are ways to protect your computer against potential security threats تهديدات:

- **Firewall**

A firewall can help protect your computer by preventing hackers or malicious software from gaining access to it.

- **Windows Update**.

Windows can routinely check for updates for your computer and install them automatically, this can help protect your computer against new viruses and other security threats. To ensure that you receive these updates as quickly as possible, turn on automatic updating.

- **Virus protection**.

Antivirus software can help protect your computer against viruses, worms, and other security threats. A computer **worm** is a *standalone malware computer program that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it*. Unlike a computer **virus**, it does *not need to attach itself to an existing program*. Worms almost always *cause at least some harm to the network, even if only by consuming bandwidth,* whereas viruses almost always *corrupt or modify files on a targeted computer*.

- **Spyware and other malware protection**.

Antispyware software can help protect your computer from spyware and other potentially يحتمل أن تكون unwanted software. **Malware** البرمجيات الخبيثة is *software designed to damage a computer system without the owner's knowledge or agreement*. Malware is short for malicious software and includes computer viruses, spyware, worms, and Trojan horses, or any other unwanted or malicious software. **Spyware** برامج التجسس is a *type of malware that can be installed on computers to collect information about users without their knowing*, these programs can also *collect personal information and change settings stored on a user's computer.*

Manage security settings with Action Center

Action Center checks several security and maintenance-related items of your computer that help indicate your computer's overall performance. When the status of a monitored item changes (for example, your antivirus software becomes out of date) Action Center notifies you with a message in the notification area on the taskbar, the status of the item in Action Center changes color to reflect the severity of the message, and an action is recommended.

Action Center * *manages firewall settings, Windows Update, anti-malware software settings, Internet security, and User Account control settings.*

Action Center also * *monitors computer maintenance settings and provides links to troubleshooters and other tools that can help fix problems*.

To change which items Action Center checks:

1. Click to open Action Center.
2. Click Change Action Center settings.
3. Select a check box to make Action Center check an item for changes or problems, or clear a check box to stop checking the item.
4. Click OK.

Use Windows Defender

Use Windows Defender to prevent malicious software, like spyware or viruses, from infecting your computer.

Windows Defender is antispyware software that's included with Windows and runs automatically when it's turned on. Using antispyware software can help protect your computer against spyware and other potentially unwanted software.

Windows Defender offers two ways to help keep spyware from infecting your computer:

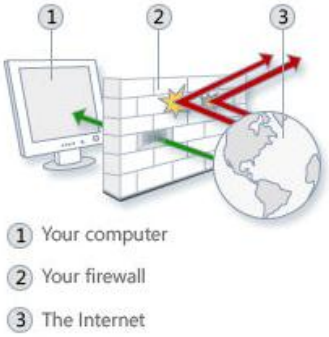
- *Real-time protection*. Windows Defender alerts you when spyware attempts to install itself or to run on your computer. It also alerts you when programs attempt to change important Windows settings.
- *Scanning options*. You can use Windows Defender to scan for spyware that might be installed on your computer, to automatically remove anything that's detected during a scan.

Use a firewall

A **firewall** is *software or hardware that checks information coming from the Internet or a network and then either turns it away or allows it to pass through to your computer*. In this way, a *firewall helps prevent hackers and malicious software from gaining access to your computer*.

Even if you think there's nothing on your computer that would interest anyone, a worm could completely disable your computer, or someone could use your computer to help spread worms or viruses to other computers without your knowledge.

Windows Firewall is built into Windows and is turned on automatically.



If you run a program such as an messaging program or a multiplayer network game that needs to receive information from the Internet or a network, the firewall asks if you want to block or unblock (allow) the connection. If you choose to unblock the connection, Windows Firewall creates an exception so that the firewall won't bother يزعج you when that program needs to receive information.

Allowing a program to communicate through the firewall, sometimes called unblocking, when you allow a particular program to send information through the firewall.

By default, most programs are blocked by Windows Firewall to help make your computer more secure. To work properly, some programs might require you to allow them to communicate through the firewall. Here's how to do that:

1. Click to open Windows Firewall.
2. In the left pane, click Allow a program or feature through Windows Firewall.

What are the risks of allowing programs through a firewall?

When you add a program to the list of allowed programs in a firewall, or when you open a firewall port, you ***allow a particular program to send information to or from your computer through the firewall***. Allowing a program to communicate through a firewall (sometimes called unblocking) is like making a punch in the firewall.

Each time you open a port or allow a program to communicate through a firewall, your computer becomes less secure. The more allowed programs or open ports your firewall has means there are more chances for hackers or malicious software to spread a worm, access your files, or use your computer to spread malicious software to others.

It's generally **safer** to add a program to the list of allowed programs than to open a port. If you *open a port*, it stays open until you close it, whether or not a program is using it. If you *add a program to the list of allowed programs*, the hole is open only when needed for a particular communication.

To help decrease your security risk:

- Only allow a program or open a port when you really need to, and remove programs from the list of allowed programs or close ports that you no longer need.
- Never allow a program that you don't recognize to communicate through the firewall.

Windows Firewall is on by default. To make sure it hasn't been turned off, follow these steps:

1. open Windows Firewall.
2. In the left pane, click Turn Windows Firewall on or off. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.
3. Below each network location type, click Turn on Windows Firewall, and then click OK. We recommend that you turn on the firewall for all network location types.

What are some of the things that a firewall can't prevent?

- E-mail viruses

E-mail viruses are attached to e-mail messages. A firewall can't determine the contents of e-mail messages, so it can't protect you from these types of viruses. You should use an antivirus program to scan and delete suspicious مشبوه attachments from an e-mail message before you open it.

- Phishing scams

Phishing الخداع is a technique used to trick computer users into revealing الكشف personal or financial information, such as a bank account password. A common online phishing scam احتيال starts with an e-mail message that appears to come from a trusted موثوق source. Firewalls can't determine the contents of e-mail messages, so they can't protect you from this type of attack.